

Missouri Department of Health and Senior Services

**HIV/AIDS Surveillance
Confidentiality and Security Manual**

October 2003

TABLE OF CONTENTS

**Missouri Department of Health and Senior Services
HIV/AIDS SURVEILLANCE
CONFIDENTIALITY AND SECURITY MANUAL
October 2003**

Preface

I. General Background and Assurances	1
A. Definitions	1
B. Legal Background	2
1. Federal Regulations	2
2. State Reporting Regulations	2
C. Confidentiality Assurances	4
1. Signing of Confidentiality Oath	4
2. Designation of ORPs and Responsibilities	4
3. Delineation of Surveillance Staff Responsibilities	6
4. Displaying of Employee Identification Badges	6
5. Administration of Performance Appraisals	6
6. Evaluation of Confidentiality/Security at HIV/AIDS Contractual Sites	6
7. Description of Penalties for Unauthorized Disclosure	6
8. Training for HIV/AIDS Confidentiality/Security	7
II. Physical Security	7
A. Building/Restricted Access Area Security	7
1. MDHSS/OoS	7
2. SLCHD	8
3. KCHD	8
B. Office/Surveillance Unit Security	9
1. Retention of Hard Copy Files	9
2. Keys to Hard Copy Storage	9
III. Computer Security	9
A. Database Security	9
B. PC Workstation Security	10
IV. Data Confidentiality and Security	11
A. Release of Data to Non-HIV/AIDS Surveillance Staff	11
B. Transfer of HIV/AIDS Surveillance Data	14
1. Contractors	14
2. CDC	14
C. Authorized Statewide HIV/AIDS Surveillance Staff	14
D. Back-ups of HIV/AIDS Surveillance Data	14

E. Disposal of HIV/AIDS Surveillance Data	15
F. Photocopying/Printing of HIV/AIDS Surveillance Data	15
V. Rapid Communication.....	15
A. Electronic.....	15
1. Facsimile	15
2. E-mail.....	16
B. Mail.....	16
1. Incoming.....	16
2. Outgoing.....	16
C. Telephone.....	16
1. Incoming.....	16
2. Outgoing.....	16
VI. Field Activities.....	17
A. Confidential Materials Transported to the Field	17
1. Line-listings	17
2. Lap-Tops	17
B. Transportation of Confidential Materials.....	17
C. Additional Field Security Protocols	17
VII. Procedures for Systematic Review of HIV/AIDS Security and Confidentiality Practices.....	18

Missouri Department of Health and Senior Services
HIV/AIDS SURVEILLANCE PROGRAM
CONFIDENTIALITY AND SECURITY MANUAL
REVISED OCTOBER 29, 2003

PREFACE

Within the state of Missouri, three HIV/AIDS surveillance units located in Jefferson City, Kansas City, and St. Louis City are responsible for implementing and operating comprehensive HIV/AIDS surveillance programs to reduce the spread of HIV infection and its impact on at-risk populations. Jefferson City is the administrative headquarters for all state surveillance activities and conducts surveillance in the Outstate area (108 counties). Kansas City conducts surveillance in a nine county region that includes four counties in Kansas. St. Louis City conducts surveillance in St. Louis City and St. Louis County, Missouri. Surveillance program activities guide prevention policy decisions, target prevention resources, and assist in evaluating prevention and treatment activities. All three surveillance units collaborated to develop this document that is intended to provide guidelines for management of confidential patient information within the context of all state surveillance activities.

This manual serves as the official confidentiality security policy of the Missouri Department of Health and Senior Services (DHSS) that pertains to HIV/AIDS data. These policies encompass all agencies that contract with the DHSS.

I. GENERAL BACKGROUND AND ASSURANCES

A. DEFINITIONS

1. **AIDS:** Acquired Immune Deficiency Syndrome.
2. **Confidential Information/Material:** All HIV/AIDS information is inherently confidential and is considered as some of the most confidential information managed by state and local health departments. Confidential information is considered as any information that could either directly (e.g., patient identifiers) or indirectly (e.g., small cell aggregate data) lead to the identification of a person reported with HIV/AIDS, or any other person whose identity was learned through a case investigation, case report, personal interview, database, or research study.
3. **Contractor (Contractual Employees/Agreements):** Entities funded to perform HIV/AIDS case surveillance through contractual agreements with DHSS. Current relationships exist with Kansas City Health Department (KCHD) and St. Louis City Department of Health and Hospitals (SLCHD).
4. **HIV:** Human Immunodeficiency Virus.

5. **HARS (HIV/AIDS Reporting System):** National, statewide, and local database for conducting HIV/AIDS case surveillance.
6. **Immediately:** With respect to reporting all breaches or suspected breaches of confidentiality (whether local health department to state health department or state health department to CDC), immediately is defined as within the same working day. If an event occurs late in a working day, the statewide and/or local ORPs are to be notified after normal working hours as soon as possible after the event occurs.
7. **Office of Surveillance (OoS):** This organization performs statewide surveillance for communicable, zoonotic, and environmental health conditions and is located organizationally within the Division of Environmental Health and Communicable Disease Prevention (EHCDP), Missouri Department of Health and Senior Services (DHSS) central office. OoS is responsible for conducting all statewide HIV/AIDS surveillance activities.
8. **Overall Responsible Parties (ORPs):** Designated individuals at DHSS and local contractual sites who are ultimately responsible for the security and confidentiality of HIV/AIDS surveillance information.
9. **Security (Secured):** All measures implemented to prevent access to confidential material by unauthorized individuals as described in this document. Examples of security include physically secured facilities, restricted access areas, password-protected databases, and HIV/AIDS surveillance staff training.
10. **Unauthorized Release/Disclosure of HIV/AIDS Surveillance Information:** All release/disclosure of HIV/AIDS surveillance information not authorized by the ORP as defined in section IV, A and C of this manual.

B. LEGAL BACKGROUND FOR SECURITY/CONFIDENTIALITY OF HIV/AIDS SURVEILLANCE INFORMATION

1. **Federal Regulations.** At the national level, HARS is protected by a Federal Assurance of Confidentiality of Public Health Service Act, 42 U.S.C. 242k and 242m(d), that prohibits disclosure that could be used to directly and indirectly identify patients.
2. **State Reporting Regulations.** At the state level, multiple regulations dictate HIV/AIDS reporting, security/confidentiality, and are described below:
 - a. **Physician Reporting-19 CSR 20-26.040.** Physicians or their designates are required to report all conditions listed in 19 CSR 20-20.020 including HIV infection as indicated by HIV antibody testing (reactive screening test followed by a positive confirmatory test), HIV antigen testing (reactive screening test followed by a positive confirmatory test), detection of HIV nucleic acid (RNA or DNA), HIV viral culture, or other testing which indicates

HIV infection; newborn infants whose mothers are infected with HIV; HIV test results (including both positive and negative results) from children less than two years of age whose mothers are infected with HIV; AIDS; CD4 lymphocyte counts; and HIV viral load measurements. Providers are protected from any civil liability for reporting under RSMo. 191.656, Subsection 7.

- b. Laboratory Reporting-19 CSR 20-20.080.** Laboratories are required to report any positive test or any test indicative of conditions listed in 19 CSR 20-20.020 including the above tests for HIV infection, AIDS, CD4 lymphocyte counts, and viral load measurements.
- c. Exemptions to Reporting-19 CSR 20-26.040.** Exemptions from HIV/AIDS case reporting include: (1) all research institutions obtaining Institutional Board Approval (IRB) for a specific study with notification of the board's approval submitted to the department in writing prior to commencement of study; or (2) where prohibited by federal law or regulation.
- d. State Statutes which Address Authorized Release of Surveillance Information.**

Specific entities to which HIV/AIDS surveillance data can be released are described in section IV, A and C.

 - 1). RSMo.191.656.** HIV/AIDS patient information can only be released to public employees with a need-to-know in order to perform their duties or private employees entrusted with patient care. Additional exceptions are outlined Subsection 2. (1) of RSMo.191.656 (Attachment 1).
 - 2). RSMo.191.677.** State statute RSMo.191.677 (Attachment 2) allows release of information by court order to allow for the prosecution of individuals who knowingly transmit HIV infection.
 - 3). RSMo.191.658.** This statute (Attachment 2a) may allow release of HIV information (if on file) to a health care practitioner providing treatment for a health care worker or law enforcement officer because of a medically significant exposure to blood or body fluids.
- e. Penalties for Unauthorized Release of Surveillance Information.**
 - 1).** Penalties for unauthorized release of HIV/AIDS patient information are classified as (1) negligent violation and (2) willful, intentional, and reckless violation. Negligent violation can result in a fine of \$1,000, including all associated court costs and reasonable attorney fees. This is in addition to other relief the court may judge appropriate. Willful violation can incur a fine of \$5,000, including exemplary damages, court costs and reasonable attorney fees, in addition to other relief the court may deem appropriate.

- 2). Breach of security and confidentiality pertaining to HIV/AIDS surveillance information may result in suspension, demotion, or termination based on the severity of the offense. Severity of offense and disciplinary action for all DHSS staff with access to HIV/AIDS surveillance information is determined by the statewide ORP. Local health department administrators may elect to consult with DHSS administrators to determine the severity of offense and disciplinary action for employees of local contractual sites. The basis for disciplinary actions for DHSS staff is found in the DHSS administrative manual, Chapter 10, Section 10.4 (Attachment 3).
- 3). Penalties for contractual programs that breach confidentiality of HIV/AIDS surveillance information may include a reduction or loss of federal and/or state funding.

C. CONFIDENTIALITY ASSURANCES

1. **Signing of Confidentiality Oath.** All statewide surveillance staff and non-surveillance staff authorized to access HIV/AIDS surveillance information sign a health department confidentiality statement upon hire. In addition, all surveillance staff and other staff who have access to confidential data (e.g., STD Disease Intervention Specialists, Tuberculosis Control staff, designated information systems specialists in DHSS and in contractual sites) annually sign a confidentiality oath pertaining to HIV/AIDS surveillance information (Attachments 4, 5, 6, 7, and 8) and receive a confidentiality packet as described in this section, number 8. The signed (original) confidentiality statement is retained in the employee’s personnel file and a copy is given to the employee.

Figure 1. Confidentiality Assurances

- Confidentiality Oaths
 - Overall Responsible Parties (ORPs) and Responsibilities
 - Surveillance Staff Responsibilities
 - Employee Identification Badges
 - Performance Appraisals
 - Contractual Staff
 - Penalties for Unauthorized Disclosures
 - Training

2. **Designation of Overall Responsible Parties (ORPs) and Responsibilities.** DHSS has identified statewide (Figure 2) and contractual (Figure 3) Overall Responsible Parties (ORPs) who are ultimately responsible for the confidentiality and security of HIV/AIDS surveillance information.

Figure 2. Statewide ORPs

- Statewide:**

(Primary):
Bryant McNally, JD, MPH, Director
Division Environmental Health and
Communicable Disease Prevention

(Secondary):
Garland Land, MPH, Director
Center for Health Information
Management and Epidemiology

Statewide ORPs: Specific responsibilities of the statewide ORPs include:

- a. Exercising the authority to make decisions about the overall HIV/AIDS surveillance operation that affect how surveillance information is collected, stored, analyzed, released, and disposed. Decisions also include which programs outside of HIV/AIDS surveillance

are authorized to access surveillance data for public health purposes. This includes both DHSS central office and contractual sites.

- b.** Collaborating closely with the Program Manager (Yelena Friedberg) and Chief, Office of Surveillance (Lyn Konstant) to annually certify that all CDC program requirements are met. Annually completing CDC’s certification form (Attachment 9).
- c.** Collaborating closely with Y. Friedberg and L. Konstant to immediately report all breaches of confidentiality to the Chief of the Reporting and Analysis Section (Dr. Lisa Lee), HIV Incidence and Surveillance Branch, CDC.
- d.** Collaborating with Y. Friedberg and L. Konstant to take appropriate disciplinary action toward central office surveillance staff and surveillance contractual entities that breach the confidentiality of HIV/AIDS surveillance information. The statewide ORP will also collaborate with managers of other DHSS programs whose employees breach confidentiality of HIV/AIDS surveillance information to establish appropriate disciplinary action.

State and local health department administrators will consult with their Department’s General Counsel to determine whether a breach warrants reporting to local and state law enforcement agencies.

Local ORPs:

Based on the fact that SLCHD and KCHD are contractual, remote HARS sites, DHSS is requesting that these health departments designate an individual to serve as the ORP for their respective surveillance jurisdictions (Figure 3). Local ORP responsibilities include:

Figure 3. Local ORPs

<p>SLCHD: Akan Ukoennin, Chief Communicable Disease Program</p> <p>KCHD: Ron Griffin, MPH, Chief Division of Communicable Disease and Prevention</p>
--

- a.** Certifying annually that all CDC program requirements are met for their surveillance jurisdiction. Annually completing DHSS’s certification form (Attachment 10).
- b.** Assuring ongoing jurisdiction adherence to all policies/procedures in Missouri’s *HIV/AIDS Confidentiality and Security Manual*.
- c.** Collaborating closely with L. Konstant and Y. Friedberg to immediately report and resolve all breaches of confidentiality pertaining to HIV/AIDS surveillance data within their surveillance jurisdiction.
- d.** Ensuring that all staff managing HIV/AIDS surveillance information are appropriately trained in all aspects of security and confidentiality.

3. Delineation of Surveillance Staff Responsibilities. Surveillance staff has the following general responsibilities pertaining to the security and confidentiality of HIV/AIDS surveillance information:

- a. Challenging unauthorized users of HIV/AIDS surveillance data. Authorized users and authorized use of HIV/AIDS surveillance information are defined in section IV of this manual, A and C.
- b. Immediately reporting all suspected breaches of confidentiality to the statewide ORP or designate. DHSS central office surveillance staff should report all breaches or suspected breaches of confidentiality to L. Konstant or Y. Friedberg. Staff in local contractual sites should report all breaches or suspected breaches of confidentiality to their designated local ORP who will then immediately notify the statewide ORP or designate.
- c. Exercising good judgment in the daily management of HIV/AIDS surveillance information. From time to time, confidentiality and security issues related to HIV/AIDS surveillance data may arise that are not specifically addressed in this manual. When these issues arise, surveillance staff is responsible for notifying the statewide ORP (or local ORP for contractual sites) whom can provide the necessary guidance related to these issues.
- d. Ensuring confidentiality of individual surveillance workstations.

Specific surveillance staff responsibilities pertaining to security/confidentiality of surveillance data are listed in the “Workplace HIV/AIDS Security Checklist” (Attachment 11).

- 4 Displaying of Employee Identification Badges.** HIV/AIDS surveillance staff statewide is required to display identification badges specific to their health department(s). These badges are required to be worn at all times when surveillance staff are working within the surveillance unit and also when conducting official activities away from the surveillance unit.
- 5. Administration of Performance Appraisals.** Confidentiality is listed as a job component on all OoS and contractual staff performance appraisals.
- 6. Evaluation of Confidentiality/Security at HIV/AIDS Contractual Sites.** Assurance of confidentiality is listed in annual HIV/AIDS surveillance contracts with the SLCHD and KCHD. OoS conducts biannual site visits with contractors to evaluate delivery of service, one area being confidentiality and security of HIV/AIDS surveillance information.
- 7. Description of Penalties for Unauthorized Disclosure of HIV/AIDS Surveillance Information.** Penalties for unauthorized disclosure of HIV/AIDS patient information are outlined in I.,B.,2.,d.

8. Training for HIV/AIDS Confidentiality/Security

- a. **New Employee Orientation.** All new surveillance staff and non-surveillance staff authorized to access HIV/AIDS surveillance information are given a confidentiality orientation and are provided the following items:
- *HIV/AIDS Security and Confidentiality Manual*
 - DHSS Rules Pertaining to HIV/AIDS (including penalties for unauthorized disclosure)
 - “Workplace HIV/AIDS Security Checklist”
 - HIV/AIDS Surveillance Program Confidentiality Statements

During the orientation, all new surveillance staff is thoroughly trained on the methodology of HIV/AIDS surveillance including protocols for HIV/AIDS security/confidentiality. All training occurs before administrative access is granted to confidential information. Dates of security orientation are documented in each employee’s personnel file.

- b. **Annual Updates/Trainings.** Confidentiality updates/reviews are held annually during one of the statewide HIV/AIDS surveillance meetings. Updates allow for sharing of information regarding confidentiality/security including discussion of new policy, review of existing policy, review of CDC program requirements, discussion of areas of perceived weakness within the statewide program, and discussion of contractual and individual penalties for unauthorized disclosure of confidential information. All non-surveillance staff authorized to access surveillance information is also provided confidentiality and security training on a periodic, established basis.
- c. **Other Trainings.** Surveillance staff statewide attend all CDC recommended or required confidentiality trainings.

II. PHYSICAL SECURITY

A. BUILDING/RESTRICTED ACCESS AREA SECURITY

Access to all restricted areas is limited to surveillance staff or other authorized individuals (e.g., program administrators, data managers) who have a need for access. Keys and/or electronic access cards are issued to surveillance staff upon hire and are surrendered to designated administrative staff upon either resignation or termination.

1. **Office of Surveillance (OoS).** OoS is located in one of three buildings operated by DHSS. Access to each building during normal business hours (defined as 6:30 am to 5:30 pm Monday through Friday) is through one entrance. All visitors are required to register at the front information desk and to display a visitor identification badge. OoS (and thus the HIV/AIDS surveillance unit) is located within the EHCDP work area. This work area requires electronic

access through two additional doors. OoS staff must accompany visitors in order to enter the unit. Outside windows are secure. There is no dedicated area for performing HIV/AIDS surveillance activities; however, HARS and other confidential databases are housed on a confidential LAN server located within the DHSS Office of Information Systems (OIS) area, not on individual workstations. OIS is located in a separate building from the EHCDP work area and the fileserver is located within an electronically secured room with limited numbers of information systems administrators granted security clearance to this room. All DHSS entrances in addition to the EHCDP work area also require electronic access after hours and on weekends of which only a limited number of individuals have access (including cleaning crews). In the event that an access card is lost or stolen, it is immediately reported to the EHCDP Assistant Director (S. Jenkins) who is responsible for reporting the lost/stolen card to the security company.

2. **St. Louis City Department of Health and Hospitals (SLCHD).** The HIV/AIDS surveillance unit is located within the Metropolitan St. Louis AIDS Program on the fourth floor of the SLCHD. Therefore, the unit is not accessible by window. The surveillance unit is a restricted access area with double-locked doors. Both the building and the unit are locked after normal working hours (defined as 8:00 am to 5:00 pm, Monday through Friday). A security guard is posted in the building twenty-four (24) hours a day and all authorized health department staff is required to sign-in for access after normal working hours. The surveillance unit is locked if no one is present within the unit. Cleaning crews do not access the surveillance unit after normal working hours. The LAN fileserver for HIV/AIDS surveillance information is located in a double-locked service room on the seventh floor of the health department, of which several data administrators (information specialists) have access. The office is locked when vacant.
3. **Kansas City Health Department (KCHD).** The HIV/AIDS surveillance unit is located in the Communicable Disease Prevention Unit on the second floor of the KCHD. All outside windows are secure. All health department visitors are required to register at the information desk and to display a visitor's identification badge. Security guards are posted in the health department twenty-four hours daily and security cameras monitor physical grounds at all times. The Communicable Disease Prevention unit is a restricted access area and is locked during normal working hours (defined as 8:00 am to 5:00 pm., Monday through Friday); however, there is no dedicated area for performing HIV/AIDS surveillance activities. The two terminals for conducting surveillance activities are located in a cubicle-sectioned corner of the Communicable Disease Prevention Unit. The LAN fileserver is located within a locked room on the fourth floor and maintained by the data administrator who is the only person who has access (in addition to cleaning crews). HARS and other confidential databases are not maintained on individual workstations. All entrances to the KCHD require electronic access after hours and on weekends of which only four (4) individuals from the Communicable Disease Prevention Unit have access. In addition, a key is required to gain access to the unit itself.

B. OFFICE/SURVEILLANCE UNIT SECURITY

1. Retention of Hard Copy Files

a. All surveillance units retain hard copy files of HIV/AIDS surveillance information. All hard copy information is stored in locked filing cabinets and is accessible only by HIV/AIDS surveillance staff. All original hard copy files are housed in locked filing cabinets at the DHSS central office in Jefferson City.

a. Hard copy documents are concealed or locked up when employees are absent from individual workstations for even brief periods of time.

2. **Keys to Hard Copy Storage.** Designated staff in each surveillance unit retains the keys to hard copy storage. However, all surveillance staff is responsible for insuring security of their individual workstations, including appropriate storage of hard copy files.

III. COMPUTER SECURITY

A. DATABASE SECURITY

1. HARS is the primary database for HIV/AIDS surveillance tracking. Other supplemental databases (e.g., death certificate, pending case, d-base 5.0) are internally designed and used for epidemiological tracking. Access to all databases is restricted to HIV/AIDS surveillance personnel via password protection.

2. All surveillance units have information system specialists (data administrators) responsible for maintaining all network and database security and integrity. In the DHSS central office, these individuals are organizationally located within and outside of the HIV/AIDS surveillance unit. In St. Louis and Kansas City, these individuals are organizationally located outside of the HIV/AIDS surveillance unit (e.g. health department director's office).

3. All surveillance units possess different configurations for network security and are outlined in Figure 4. In no surveillance unit is HARS maintained on individual workstations.

Figure 4. HIV/AIDS Surveillance Network Configuration by Surveillance Unit

MDHSS:	Connected to DHSS LAN (network), DHSS Office of Information Systems (OIS) administers fileserver containing HIV/AIDS surveillance information. Surveillance utilizes trustee rights to confidential volume on fileserver.
St. Louis City:	Connected to SLCHD LAN (network), the STD Control Program and the HIV/AIDS Surveillance Program share a confidential server.
Kansas City:	Connected to KCHD LAN (network), surveillance utilizes trustee rights to confidential volume on fileserver.

B. PC WORKSTATION SECURITY

1. All surveillance staff is responsible for protecting his/her workstation (terminal) containing HIV/AIDS surveillance information. This includes protecting individual passwords that would allow access to confidential information/data.
2. Terminals for all statewide HIV/AIDS surveillance staff are single password protected. Passwords in all surveillance jurisdictions are at least a minimum of five characters. On an established basis in each jurisdiction, users change passwords to insure database security. Access to HARS and other confidential databases are restricted to HIV/AIDS surveillance personnel via group access authority and network password protection.
3. All surveillance staff log off the network at the end of each day or when leaving the office for extended periods of time (defined as 2 hours or more). In the event a user fails to log out, networks at SLCHD, KCHD and DHSS automatically log off users after a specified time.
4. OoS terminals utilize privacy screens due to workstation configurations.
5. At DHSS, retention of any confidential information (other than the information contained in HARS) is maintained on secured drives. At KCHD, confidential information in addition to HARS is stored in d-base (a major supplemental database). Also, the secured drive is used to store nightly back-ups of HARS. Secured drives are protected, and access is restricted to the user group. The data manager or designated information specialists of DHSS, SLCHD and KCHD also have access. Secured drives are not needed at SLCHD due to network configuration.
6. All disks and computer hard drives are cleaned prior to surplus with Norton's WipeInfo (Government Erase). At DHSS, DHSS Office of Information Systems (OIS) staff prior to surplus also checks all hard drives for confidential information.
7. Anti-virus software is installed on all terminals at DHSS, SLCHD, and KCHD. Surveillance staff is responsible for reporting all computer viruses or suspected computer viruses to their designated information systems staff.
8. All surveillance system hardware (fileservers) is located in areas that are adequately regulated with respect to temperature to avoid software/hardware damage.

IV. DATA CONFIDENTIALITY AND SECURITY

A. RELEASE OF DATA TO NON-HIV/AIDS SURVEILLANCE STAFF

1. All data released is in accordance with RSMo.191.656, 191.677 and 191.658 that provides general guidelines for the release of HIV/AIDS surveillance information. This manual approved by the statewide ORP, lists specific protocols and policies for the release of HIV/AIDS surveillance information.
2. All surveillance staff is required to exercise discretion when releasing any surveillance data. Surveillance staff should consult with the local or statewide ORP (or designate) if they have questions pertaining to release of HIV/AIDS surveillance information.
3. All surveillance information pertaining to a specific HIV/AIDS case may be released to known, authorized providers (including infection control practitioners) directly involved in the health care of a patient.
4. All surveillance information may be released to authorized out-of-state surveillance staff for the tracking of a patient within their jurisdiction.
5. Confidential information may be released to other agencies within or outside DHSS who require such information to perform their job responsibilities (Figure 5).

Figure 5. Agencies in Missouri Obtaining Confidential HIV/AIDS Information

- STD Program
- TB program
- Medicaid Waiver Program
- HIV Case Management
- State and Local Prosecuting Agencies

a. Sexually Transmitted Disease Control Program.

In Missouri, HIV/AIDS surveillance data are linked with partner notification activities for sexually transmitted diseases including HIV. Designated surveillance staff provide in-state and local contractual Disease Intervention Specialists (DIS) with only the patient information (demographic, clinical, and risk) needed to perform an effective field investigation. Surveillance staff also shares information with out-of-state STD Control programs for the same reason. The efforts of DIS identify contacts to known cases and therefore can potentially identify new cases of HIV infection. When required, DIS also has an integral role in resolving NIR (no-identified risk) investigations. Exchange of information between HIV/AIDS surveillance staff and DIS staff is bilateral and occurs on both the state and local levels.

- #### b. Tuberculosis Control Program.
- In the DHSS central office on a quarterly basis, names and dates of birth of all tuberculosis infection, tuberculosis disease and mycobacterium other than tuberculosis (MOTT) cases are matched electronically to names and dates of birth of cases in HARS. Designated HIV/AIDS surveillance staff conducts the match. If an individual has dual diagnoses (i.e., TB/MOTT and/or HIV/AIDS), the diagnosis and

RVCT number is noted on the patient record in both the tuberculosis and HARS registries. Hardcopy HIV/AIDS case reports are not shared with the tuberculosis program staff.

The KCHD HIV/AIDS Surveillance Program obtains names, dates of birth, and diagnosis of persons with tuberculosis disease or MOTT from the local tuberculosis program. After HARS is record searched and the appropriate co-morbidity updated in HARS, the tuberculosis program is then notified of the dual diagnosis of either HIV or AIDS. The tuberculosis program uses a numerical code to indicate those persons with co-morbidity (a three digit number which is used in place of the words “HIV or AIDS”).

The SLCHD HIV/AIDS Surveillance Program does not receive any information from their local tuberculosis program. Tuberculosis disease and MOTT updates are received on hardcopy from Jefferson City. This information is shredded after local entry into HARS.

- c. Missouri Medicaid Waiver Program.** Upon request, designated HIV/AIDS surveillance staff confirms the HIV diagnosis of individuals receiving services under the Medicaid Waiver Program and report the status to designated Medicaid Waiver staff. Only confirmation of either HIV/AIDS diagnosis is provided to Medicaid waiver staff, no additional surveillance information. Medicaid information can also be a potential case finding/validation source for the Missouri surveillance program. Release of this information only occurs on the state level.
- d. HIV Case Management Program.** Upon request, HIV/AIDS surveillance staff verifies the diagnosis of individuals who apply for Missouri HIV case management services. Case management links HIV diagnosed clients to care, community resources, and information. Confirmation of HIV/AIDS diagnosis (including appropriate laboratory information, CD4 counts, viral loads, and opportunistic infections) is provided to designate case management staff. Additional surveillance information (e.g., partner notification activity) may be provided if requested to assist with comprehensive patient management. Case management is also a valuable case finding/validation source for the Missouri surveillance program. Release of this information occurs on both state and local levels.
- e. State and Local Prosecuting Agencies.** Upon request, HIV/AIDS surveillance information can be released to state and local prosecuting attorneys to enforce RSMo. 191.677. Release is coordinated by the Chief, OoS with DHSS General Counsel. The only information released to prosecutors is laboratory history to verify the status of the prosecuted individual. Release of information occurs only on the state level.
- 6. DHSS does not release HIV/AIDS surveillance information to law enforcement officials (e.g., defense attorneys, prosecuting attorneys, and detectives) not described under the scope of RSMo.191.677 without a subpoena or court order, depending on the exact nature of the request. The statewide ORP or designate collaborates closely with the DHSS Chief Counsel to respond to all named-identifier requests from law enforcement. DHSS Chief Counsel collaborates with the State’s Attorney General’s Office to resist all such release of HIV/AIDS**

surveillance information. Local contractual agencies are required to refer all requests from law enforcement to the statewide ORP or designate.

7. According to state statute, RSMo.191.658, a health care practitioner, providing medical treatment for a health care worker or law enforcement officer because of a medically significant exposure to blood or other body fluids that occurred in the course of the worker's or officer's employment, may request from the department of health, information regarding the HIV infection status of the source individual.

A protocol has been established for operationalizing the requirements of this statute and to reduce to a minimum the number of times the state registry is used to determine the status of a source individual. Local contractual agencies and central office staff are required to refer all requests from providers to the statewide ORP or designate. These requests are then routed to one of the designated state HIV consultants (e.g., consultant community health nurse, medical epidemiologist) who will determine if a significant exposure, as defined in the law, has occurred and if HIV information on the source individual is essential in providing necessary medical treatment. The caller will be provided with appropriate treatment recommendations and other medical information (e.g., assure the exposed individual is evaluated for hepatitis B and C as well as HIV, referring to CDC recommendations for post-exposure prophylaxis).

If the information collected meets the criteria set forth in the law and it is determined that the source person's HIV status is needed in order to determine or encourage ongoing appropriate treatment for the exposed individual, information on the exposed individual will be obtained (e.g., name, date of birth, race). This information will be referred to authorized staff in OoS who have access to the HIV/AIDS database (Section C., Figure 4). Only those individuals with access to the HIV/AIDS database will know if the source patient is infected with HIV and will have the responsibility to notify the provider of the results.

8. State statute (RSMo.191.689) requires school notification of children with HIV infection, only after a school has adopted a policy consistent with recommendations of CDC on school children that test positive for HIV. In view of concerns related to patient confidentiality, the HIV/AIDS surveillance program does not operationalize the statute.
9. Named HIV data are not released to researchers unless they sign the DHSS HIV/AIDS surveillance program confidentiality statement and are conducting a DHSS Institutional Review Board (IRB) approved project.
10. De-identified HIV/AIDS surveillance data sets are provided to statewide and local epidemiologists for the analysis of HIV/AIDS surveillance data.
11. The statewide HIV/AIDS surveillance program exercises great caution in public release of numerical, small cell data that could either directly or indirectly lead to the identification with a person infected with HIV/AIDS. Several independent variables (e.g., risk factor, race, age) could lead to the direct/indirect identification of a person with HIV/AIDS and should be

carefully evaluated in view of the total population of the jurisdiction under observation including racial and risk distribution/prevalence. For the central office program, no small cell data are released without consent from the Program Manager and/or the Chief of the office. In contractual sites, no small cell data are released without the consent of the local ORP or designate.

B. TRANSFER OF HIV/AIDS SURVEILLANCE DATA

1. **Contractors.** HIV/AIDS Surveillance contractual sites monthly transfer completed HIV/AIDS case forms and other confidential information to OoS. Transfer is performed in two forms: hardcopy and electronic. Regarding hardcopy transfer, both contractual sites mail all hard copy data (i.e., completed HIV/AIDS case report forms, laboratory results) in double envelopes via certified mail. Both contractual sites (SLCHD and KCHD) electronically transmits cases via password protected E-mail. OoS mails all confidential hard copy information to contractors in double envelopes sent via certified mail.
2. **CDC.** OoS forwards all new and updated entries on HARS records to CDC monthly via password protected E-mail. Patient names are not forwarded to CDC.

C. AUTHORIZED STATEWIDE HIV/AIDS SURVEILLANCE STAFF WITH ACCESS TO HARS

Only authorized staff performing HIV/AIDS surveillance responsibilities has **direct** access to HARS. Authorized surveillance staff for all three units and defined functions within that unit are listed in Figure 6.

Figure 6. Statewide Personnel* with Authorized Access to HARS and Function

OoS	Statewide HIV/AIDS Research Analyst HIV/AIDS Surveillance Specialist (Outstate Core Surveillance) HIV/AIDS Database Manager (Statewide QA, Entry of Outstate Case Reports, Preparation of Statistical Reports) Two Support Staff (Laboratory Data Entry) Two Data Managers (Data Administration)
St. Louis City	HIV/AIDS Surveillance Coordinator (Preparation of Statistical Reports) HIV/AIDS Surveillance Specialist (City/County Core Surveillance) HIV/AIDS Surveillance Support (Laboratory Data Entry)
Kansas City	HIV/AIDS Surveillance Coordinator (HIV/AIDS Case Surveillance, Data Entry, Preparation of Statistical Reports)

* Systems administrators in all three areas have access to HARS for fileserver maintenance but HARS is not accessed on a routine basis.

D. BACK-UPS OF HIV/AIDS SURVEILLANCE DATA

Back-ups are performed regularly in all surveillance jurisdictions.

1. **DHSS.** At DHSS, OIS completes a full back-up of all computer volume for DHSS users once a week, with incremental back-ups daily. Data are saved on tapes that are stored in a locked room within the OIS unit. Incremental back-ups are kept for one week, full back-ups are kept for one month; the last full back-up on the last day of the month is kept indefinitely in an offsite safe which only two OIS system administrators have access.
2. **SLCHD.** At SLCHD, the surveillance support clerk backs up the HARS database on diskettes at the end of a two-week period. The same disk is used when the next back up occurs (data overwritten). The disks are stored in a filing cabinet within the locked surveillance unit.
3. **KCHD.** At KCHD, the AIDS surveillance coordinator backs up HARS nightly on a secured drive. Each nightly back-up is kept for one week and is then overwritten by the current week's data

E. DISPOSAL OF HIV/AIDS SURVEILLANCE DATA

1. All hard copy confidential information (e.g., CD4-lymphocyte, viral load reports, notes from medical record reviews) is shredded when no longer needed.
2. All disks and computer hard drives are cleaned prior to surplus with Norton's WipeInfo (Government Erase).

F. PHOTOCOPYING/PRINTING OF HIV/AIDS SURVEILLANCE DATA

Confidential information is not left unattended in common access areas and is retrieved immediately upon copying/printing.

V. RAPID COMMUNICATION

A. ELECTRONIC

1. **Facsimile.** Facsimile is used in all surveillance units to communicate confidential information. When confidential information is faxed outside the surveillance unit, all staff assures that the recipient has a dedicated facsimile line or is contacted prior to transmission. Confidential material faxed to outside sources contains a generic health department cover sheet that contains a notice of confidentiality. Neither the cover sheet nor faxed material has any direct or indirect reference to HIV/AIDS. If incoming faxes are not received within the expected time, surveillance staff contacts the sender. The KCHD HIV/AIDS surveillance program does not have a dedicated facsimile line. However, only HIV/AIDS surveillance staff retrieves faxes containing confidential information. DHSS and the SLCHD do have dedicated facsimile lines.

2. **E-mail.** E-mail may be used to transmit named identifying information to other DHSS staff or contractors using PK-zip with password protection (data encryption method). E-mail is utilized to transmit HARS data electronically from both contractual sites to DHSS. In addition, OoS transmits new and updated entries on HARS records to CDC via E-mail.

B. MAIL

1. **Incoming-** All incoming department mail is opened in the mail opening room. Four persons work in this room. These persons are required to sign the department confidentiality statement; however, the director of the department made the decision that it wasn't necessary for these individuals to sign the HIV/AIDS confidentiality statement. The mail is then opened and date stamped by these individuals. If it's considered safe mail, it's put in a slot in the safe room. When all mail is opened, and considered safe, it is then put in a gray tub and delivered to each section or office. On delivery, a designated person (office manager) in OoS signs a form stating that the mail has been delivered. The mail is then dispersed to designate HIV/AIDS surveillance staff. Senders of confidential information are instructed to address mail to the designated surveillance unit. Physicians and other case reporters are provided return envelopes stamped "confidential" for submitting case reports. The return envelopes have no direct reference to HIV/AIDS. Appropriate administrative personnel (e.g., Program Manager at KCHD and HIV/AIDS Surveillance Coordinators at SLCHD and OoS) should be notified of all mail routed to the incorrect health department program and appropriate health department staff and/or providers notified to prevent reoccurrence.
2. **Outgoing-** All outgoing mail containing patient identifiers is marked "confidential", double enveloped, and sent via certified mail. No outgoing envelopes have any direct or indirect reference to HIV/AIDS.

C. TELEPHONE

1. **Incoming-** Generic identifiers (e.g., "Department of Health and Senior Services", "This is Joe", "Office of Surveillance"), without any direct reference to HIV/AIDS, are used when answering all incoming calls. Confidential information is shared over the phone with individuals authorized to access HIV/AIDS surveillance information as listed in section IV, A and C. Specific techniques (e.g., call back verification) are recommended to determine authorized individuals.
2. **Outgoing-** Confidential information is requested via phone to perform routine HIV/AIDS surveillance activities. Messages with identifying patient identifiers are not left on voice mail systems unless there is prior confirmation of a secure line. Staff discusses confidential information only in secure areas, release information to only those individuals with a need-to-know (as defined in section IV, A and C), and always use utmost discretion.

VI. FIELD ACTIVITIES

A. CONFIDENTIAL MATERIALS TRANSPORTED TO THE FIELD

1. Line-listings

- a.** Line-listings are routinely carried into the field to perform routine HIV/AIDS surveillance activities.
- b.** Surveillance information on line listings is de-identified. Although line-listings typically contain the patient name, DOB, status (HIV or AIDS), and risk information, the status and risk information is coded either alphabetically or numerically (such as the coding system used in HARS) so as to neither directly nor indirectly identify the contents of the line-list.
- c.** Only patient information on work to be performed for that day is transported into the field.

- 2. Laptops.** Laptops are not currently used in the field for HIV/AIDS surveillance activities.

B. TRANSPORTATION OF CONFIDENTIAL MATERIALS

- 1.** All confidential materials are carried in a secured briefcase when performing field activities. Briefcases are never left unattended including in locked vehicles.
- 2.** Confidential information should always be returned to the HIV/AIDS surveillance unit at the close of each business day. Prior approval must be obtained from the HIV/AIDS surveillance coordinator when out-of-town travel or some other reason precludes the return of confidential information to the unit.
- 3.** When it is absolutely not possible to return confidential materials to the surveillance unit at the close of each business day (either because out-of town travel, emergency, or for some other reason), confidential information is always stored in appropriate places (e.g., locked hotel rooms, private residences).

C. ADDITIONAL FIELD SECURITY PROTOCOLS

- 1.** Surveillance staff always presents health department identification when performing surveillance field activities.
- 2.** All discussions pertaining to confidential information are conducted in secure, private areas. Medical record reviews are conducted as discreetly as possible.

3. Confidential information is never left in public or general access areas.

VII. PROCEDURES FOR SYSTEMATIC REVIEW OF HIV/AIDS SECURITY AND CONFIDENTIALITY PRACTICES

- A. The Program Manager has prepared a spreadsheet to evaluate statewide progress toward meeting CDC program requirements. The spreadsheet lists individual program requirements and descriptions of how they are currently being met. For those that have not been met, progress toward compliance is detailed. The spreadsheet includes all DHSS, SLCHD, and KCHD activities. The spreadsheet will be reviewed on an annual basis to insure compliance with all program requirements. Based on the review of the contents of the spreadsheet, this manual will be appropriately updated.
- B. When all changes to information systems technology are proposed (e.g., fileserver configuration changes, purchase of new equipment for CDC pilot projects), information system specialists in all surveillance units are responsible for collaborating with the program manager to prepare technical solutions. This collaboration will help ensure that in no way the security and confidentiality of HIV/AIDS surveillance data are electronically compromised.

Missouri Revised Statute

Chapter 191
Health and Welfare
Section 191.656

August 28, 2003

Confidentiality of reports and records, exceptions--violation, civil action for injunction, damages, costs and attorney fees--health care provider participating in judicial proceeding, immune from civil liability.

191.656. 1. (1) All information known to, and records containing any information held or maintained by, any person, or by any agency, department, or political subdivision of the state concerning an individual's HIV infection status or the results of any individual's HIV testing shall be strictly confidential and shall not be disclosed except to:

(a) Public employees within the agency, department, or political subdivision who need to know to perform their public duties;

(b) Public employees of other agencies, departments, or political subdivisions who need to know to perform their public duties;

(c) Peace officers, as defined in section 590.100, RSMo, the attorney general or any assistant attorneys general acting on his or her behalf, as defined in chapter 27, RSMo, and prosecuting attorneys or circuit attorneys as defined in chapter 56, RSMo, and pursuant to section 191.657;

(d) Prosecuting attorneys or circuit attorneys as defined in chapter 56, RSMo, to prosecute cases pursuant to section 191.677 or 567.020, RSMo. Prosecuting attorneys or circuit attorneys may obtain from the department of health and senior services the contact information and test results of individuals with whom the HIV-infected individual has had sexual intercourse or deviate sexual intercourse. Any prosecuting attorney or circuit attorney who receives

information from the department of health and senior services pursuant to the provisions of this section shall use such information only for investigative and prosecutorial purposes and such information shall be considered strictly confidential and shall only be released as authorized by this section;

(e) *Persons other than public employees who are entrusted* with the regular care of those under the care and custody of a state agency, including but not limited to operators of day care facilities, group homes, residential care facilities and adoptive or foster parents;

(f) As authorized by subsection 2 of this section;

(g) Victims of any sexual offense defined in chapter 566, RSMo, which includes sexual intercourse or deviate sexual intercourse, as an element of the crime or to a victim of a section 566.135, RSMo, offense, in which the court, for good cause shown, orders the defendant to be tested for HIV, hepatitis B, hepatitis C, syphilis, gonorrhea, or chlamydia, once the charge is filed. Prosecuting attorneys or circuit attorneys, or the department of health and senior services may release information to such victims;

(h) Any individual who has tested positive or false positive to HIV, hepatitis B, hepatitis C, syphilis, gonorrhea, or chlamydia, may request copies of any and all test results relating to said infections.

(2) Further disclosure by public employees shall be governed by subsections 2 and 3 of this section;

(3) Disclosure by a public employee or any other person in violation of this section may be subject to civil actions brought under subsection 6 of this

Attachment 1 (con't)

section, unless otherwise required by chapter 330, 332, 334, or 335, RSMo, pursuant to discipline taken by a state licensing board.

2. (1) Unless the person acted in bad faith or with conscious disregard, no person shall be liable for violating any duty or right of confidentiality established by law for disclosing the results of an individual's HIV testing:

(a) To the department of health and senior services;

(b) To health care personnel working directly with the infected individual who have a reasonable need to know the results for the purpose of providing direct patient health care;

(c) Pursuant to the written authorization of the subject of the test result or results;

(d) To the spouse of the subject of the test result or results;

(e) To the subject of the test result or results;

(f) To the parent or legal guardian or custodian of the subject of the testing, if he is an unemancipated minor;

(g) To the victim of any sexual offense defined in chapter 566, RSMo, which includes sexual intercourse or deviate sexual intercourse, as an element of the crime or to a victim of a section 566.135, RSMo, offense, in which the court, for good cause shown, orders the defendant to be tested for HIV, B, hepatitis C, syphilis, gonorrhea, or chlamydia, once the charge is filed;

(h) To employees of a state licensing board in the execution of their duties under chapter 330, 332, 334, or 335, RSMo, pursuant to discipline taken by a state licensing board;

The department of health and senior services and its employees shall not be held liable for disclosing an HIV-infected person's HIV status to individuals with whom that person had sexual intercourse or deviate sexual intercourse;

(2) Paragraphs (b) and (d) of subdivision (1) of this subsection shall not be construed in any court to

impose any duty on a person to disclose the results of an individual's HIV testing to a spouse or health care professional or other potentially exposed person, parent or guardian;

(3) No person to whom the results of an individual's HIV testing has been disclosed pursuant to paragraphs (b) and (c) of subdivision (1) of this subsection shall further disclose such results; except that prosecuting attorneys or circuit attorneys may disclose such information to defense attorneys defending actions pursuant to section 191.677 or 567.020, RSMo, under the rules of discovery, or jurors or court personnel hearing cases pursuant to section 191.677 or 567.020, RSMo. Such information shall not be used or disclosed for any other purpose;

(4) When the results of HIV testing, disclosed pursuant to paragraph (b) of subdivision (1) of this subsection, are included in the medical record of the patient who is subject to the test, the inclusion is not a disclosure for purposes of such paragraph so long as such medical record is afforded the same confidentiality protection afforded other medical records.

3. All communications between the subject of HIV testing and a physician, hospital, or other person authorized by the department of health and senior services who performs or conducts HIV sampling shall be privileged communications.

4. The identity of any individual participating in a research project approved by an institutional review board shall not be reported to the department of health and senior services by the physician conducting the research project.

5. The subject of HIV testing who is found to have HIV infection and is aware of his or her HIV status shall disclose such information to any health care professional from whom such person receives health care services. Said notification shall be made prior to receiving services from such health care professional if the HIV-infected person is medically capable of conveying that information or as soon as he or she becomes capable of conveying that information.

6. Any individual aggrieved by a violation of this section or regulations promulgated by the department of health and senior services may bring a civil action for damages. If it is found in a civil action that:

Attachment 1 (con't)

(1) A person has negligently violated this section, the person is liable, for each violation, for:

(a) The greater of actual damages or liquidated damages of one thousand dollars; and

(b) Court costs and reasonable attorney's fees incurred by the person bringing the action; and

(c) Such other relief, including injunctive relief, as the court may deem appropriate; or

(2) A person has willfully or intentionally or recklessly violated this section, the person is liable, for each violation, for:

(a) The greater of actual damages or liquidated damages of five thousand dollars; and

(b) Exemplary damages; and

(c) Court costs and reasonable attorney's fees incurred by the person bringing the action; and

(d) Such other relief, including injunctive relief, as the court may deem appropriate.

7. No civil liability shall accrue to any health care provider as a result of making a good faith report to the department of health and senior services about a person reasonably believed to be infected with HIV, or cooperating in good faith with the department in an investigation determining whether a court order directing an individual to undergo HIV testing will be sought, or in participating in good faith in any judicial proceeding resulting from such a report or investigations; and any person making such a report, or cooperating with such an investigation or participating in such a judicial proceeding, shall be immune from civil liability as a result of such actions so long as taken in good faith.

(L. 1988 H.B. 1151 & 1044 § 3, A.L. 1992 S.B. 511 & 556 merged with S.B. 638, A.L. 1993 S.B. 233, A.L. 1996 S.B. 858, A.L. 1999 H.B. 191, A.L. 2002 H.B. 1756)

.... These words appear twice in original rolls.

(1998) Prosecutors, judges and juries are public employees with a need to know for prosecutions pursuant to section 191.677. State v. Mahan, 971 S.W.2d 307 (Mo.banc).

Missouri Revised Statute

Chapter 191 Health and Welfare Section 191.677

August 28, 2003

Prohibited acts, criminal penalties.

191.677. 1. It shall be unlawful for any individual knowingly infected with HIV to:

- (1) Be or attempt to be a blood, blood products, organ, sperm or tissue donor except as deemed necessary for medical research;
- (2) Act in a reckless manner by exposing another person to HIV without the knowledge and consent of that person to be exposed to HIV, in one of the following manners:
 - (a) Through contact with blood, semen or vaginal secretions in the course of oral, anal or vaginal sexual intercourse; or
 - (b) By the sharing of needles; or
 - (c) By biting another person or purposely acting in any other manner which causes the HIV-infected person's semen, vaginal secretions, or blood to come into contact with the mucous membranes or nonintact skin of another person.

Evidence that a person has acted recklessly in creating a risk of infecting another individual with HIV shall include, but is not limited to, the following:

- a. The HIV-infected person knew of such infection before engaging in sexual activity with another person, sharing needles with another person, biting another person, or purposely causing his or her semen, vaginal secretions, or blood to come into contact with the mucous membranes or nonintact skin of another person, and such other person is unaware

of the HIV-infected person's condition or does not consent to contact with blood, semen or vaginal fluid in the course of such activities;

b. The HIV-infected person has subsequently been infected with and tested positive to primary and secondary syphilis, or gonorrhea, or chlamydia; or

c. Another person provides evidence of sexual contact with the HIV- infected person after a diagnosis of an HIV status.

2. Violation of the provisions of subdivision (1) or (2) of subsection 1 of this section is a class B felony unless the victim contracts HIV from the contact in which case it is a class A felony.

3. The department of health and senior services or local law enforcement agency, victim or others may file a complaint with the prosecuting attorney or circuit attorney of a court of competent jurisdiction alleging that a person has violated a provision of subsection 1 of this section. The department of health and senior services shall assist the prosecutor or circuit attorney in preparing such case, and upon request, turn over to peace officers, police officers, the prosecuting attorney or circuit attorney, or the attorney general records concerning that person's HIV-infected status, testing information, counseling received, and the identity and available contact information for individuals with whom that person had sexual intercourse or deviate sexual intercourse and those individuals' test results.

4. The use of condoms is not a defense to a violation of paragraph (a) of subdivision (2) of subsection 1 of this section.

FIRST REGULAR SESSION
[TRULY AGREED TO AND FINALLY PASSED]
HOUSE BILL NO. 271
90TH GENERAL ASSEMBLY

L0740.01T 1999

AN ACT

Relating to disclosure of information for medical treatment, with a penalty provision.

Be it enacted by the General Assembly of the state of Missouri, as follows:

Section 1. 1. As used in this section, the following terms shall mean:

- (1) "Disclose", to disclose, release, transfer, disseminate or otherwise communicate all or any part of any record orally, in writing or by electronic means to any person or entity;**
- (2) "Health care practitioner", any licensed physician, nurse practitioner or physician's assistant;**
- (3) "HIV", the human immunodeficiency virus that causes acquired immunodeficiency syndrome;**
- (4) "HIV infection", the pathological state of the human body in response to HIV;**
- (5) "Medically significant exposure", a puncture through or laceration of the skin, or contact of mucous membrane or nonintact skin with blood, tissue, wound exudate or other body fluids, including semen, vaginal secretions, cerebrospinal fluid, synovial fluid, pleural fluid, peritoneal fluid, pericardial fluid, amniotic fluid or any body fluid containing visible blood, or contact of intact skin with any such body fluids when the duration of contact is prolonged or involves an extensive area of skin;**
- (6) "Person", private individuals, private or public bodies politic, and corporations, partnerships, trusts, and unincorporated associations and their officers, directors, agents or employees;**

(7) "Source individual", the person who is the source of the blood or other body fluids to which medically significant exposure occurred.

2. A health care practitioner providing medical treatment for a health care worker or law enforcement officer because of a medically significant exposure to blood or other body fluids that occurred in the course of the worker's or officer's employment may request from the department of health information regarding the HIV infection status of the source individual. The department of health may disclose to the health care practitioner the HIV infection status of the source individual if such information is on file with the department.

3. The health care practitioner shall disclose the HIV infection status of the source individual to the exposed health care worker or law enforcement officer if, in the professional judgment of the health care practitioner, such disclosure is necessary to assure adherence to a prescribed treatment regimen.

4. No person to whom information about an individual's HIV infection has been disclosed pursuant to this section shall further disclose such results.

5. Any person who knowingly releases information in violation of this section is guilty of a class A misdemeanor.





ADMINISTRATIVE MANUAL

SUBJECT: PROBATION, PERFORMANCE APPRAISAL AND DISCIPLINE Disciplinary Action	Chapter: 10
	Section: 10.4
REFERENCES: State Personnel Division Rules Manual – 1 CSR 20-3.070	Page: 1 of 6
RSMo Chapters 36.410 and 577.520, HB 600	Revised: 9-23-03

DISCIPLINARY ACTION

I. PURPOSE:

To set forth causes for disciplinary action, including suspension, demotion or dismissal, depending upon the seriousness of the violation. However, discipline may be based upon causes other than these.

II. SCOPE:

Departmentwide.

III. POLICY:

- A. Some of the causes for disciplinary action are as follows. The list is not considered to be all-inclusive. Decisions regarding the severity of a disciplinary action are based on the seriousness or nature of the misconduct and/or prior disciplinary actions administered to the employee.
1. Has willfully violated any of the rules, regulations, policies or procedures of the Department after having been made aware of such.
 2. Has willfully violated any of the provisions of the State Merit System Law or of the rules of the Personnel Advisory Board.
 3. Is incompetent, inadequate, careless or inefficient in the performance of duties of their position (specific instances to be charged) or has failed to meet established minimum standards in the performance of such duties.
 4. Has been wantonly careless or negligent in the care of the property of the state.
 5. Has been guilty of abusive or improper treatment toward an inmate or patient of any state institution or to a person in custody, provided the acts committed were not necessarily or lawfully committed in self-defense, to protect the lives of others or to prevent the escape of anyone lawfully in custody.



ADMINISTRATIVE MANUAL

SUBJECT: PROBATION, PERFORMANCE APPRAISAL AND DISCIPLINE Disciplinary Action	Chapter: 10
	Section: 10.4
REFERENCES: State Personnel Division Rules Manual – 1 CSR 20-3.070	Page: 2 of 6
RSMo Chapters 36.410 and 577.520, HB 600	Revised: 9-23-03

6. Has some permanent or chronic physical or mental ailment or defect which incapacitates them for the proper performance of the duties of this position, including unrehabilitated alcoholism or narcotics addiction.
7. Has been habitually tardy in reporting for duty or has absented themselves frequently from duty during the course of regular working hours or has been completely absent from duty without prior or subsequent authorization for such absences.
8. Has been convicted of a felony or of a misdemeanor involving moral turpitude.
9. Has been guilty of a scandalous and disgraceful conduct while on or off duty where such conduct tends to bring the state service into public disrepute, or has exhibited behavior which adversely affects the employee's job performance, the employing agency, or both.
10. Has been guilty of abusive or improper treatment of guests or clients while on duty at any state facility or on any state land normally open to the public.
11. Has submitted a false statement of a material fact or has practiced or attempted to practice any fraud or deception in an application or examination or in otherwise attempting to secure employment subject to the provisions of these rules.
12. Has been guilty of insubordination or has failed to respond in a reasonable manner to the lawful orders or instructions of persons with duly delegated authority over the employee.
13. Has been abusive or physically violent toward other employees while on duty or in the duty area or has willfully exhibited behavior which is disruptive of the working activities of other employees.
14. Has been intoxicated or under the influence of a controlled substance while on duty except as may have been required by a licensed medical physician.
15. Has practiced or attempted to practice fraud or deception in securing or attempting to secure benefits or grants from a state agency either for himself or for another applicant.



ADMINISTRATIVE MANUAL

SUBJECT: PROBATION, PERFORMANCE APPRAISAL AND DISCIPLINE Disciplinary Action	Chapter: 10
	Section: 10.4
REFERENCES: State Personnel Division Rules Manual – 1 CSR 20-3.070	Page: 3 of 6
RSMo Chapters 36.410 and 577.520, HB 600	Revised: 9-23-03

16. Refuses to cooperate fully and truthfully with any formal or informal investigation, hearing or panel conducted by anyone within the Department or other state agency or body authorized to conduct same.
 17. Has failed to pay state income taxes or has failed to otherwise comply with the provisions of Section 577.520.1 and .2, RSMo (HB 600 2003), and DHSS Policy 15.6, Employee Obligation to Pay State Income Taxes.
- B. Any situation in which disciplinary action is being recommended or initiated should be discussed with the Office of Personnel (OP). The Incident Report form may be used to gather all relevant information for misconduct situations in which a supervisor may potentially recommend disciplinary action for an employee (see Attachment A). The supervisor should make reference to the disciplinary action in the next performance appraisal. A special performance appraisal may be initiated depending on the nature of the situation.
- C. It is the responsibility of supervisors and managers to administer discipline in a consistent, impartial and constructive manner and to prepare and maintain documentation to support disciplinary actions. Discipline may be imposed by an employee's immediate supervisor or other management staff in the chain of command.

IV. GUIDELINES FOR DISCIPLINARY ACTION

There may be situations which require the supervisor to deal with an employees' performance or behavior by recommending a disciplinary action. Such actions should be taken in consultation with the chain of command and the OP. Documentation is a key factor to be considered in any disciplinary action. Documentation needs to be clear, timely and behaviorally specific. Documentation for any of the types of disciplinary actions in Section V should include the following:

1. Was the employee aware of the rule, policy, procedure or expectation at the time of the violation?



ADMINISTRATIVE MANUAL

SUBJECT: PROBATION, PERFORMANCE APPRAISAL AND DISCIPLINE Disciplinary Action	Chapter: 10
	Section: 10.4
REFERENCES: State Personnel Division Rules Manual – 1 CSR 20-3.070	Page: 4 of 6
RSMo Chapters 36.410 and 577.520, HB 600	Revised: 9-23-03

2. Has the violation or incident been thoroughly investigated to determine the facts? Do you have written statements from witnesses? (The Incident Report form will assist you with this.)
3. What did or did not happen? Use words to paint a very clear picture. Explain in simple, objective, precise language exactly what happened. Specific dates, times, places and circumstances of the event should also be recorded. The Incident Report is a useful tool to use in gathering information.
4. What is the employee's perspective with regard to the occurrence? Get the employee's side of the story in writing.
5. Why is this event being documented? Explain how the event relates to and affects the employee's performance, the performance of others, and the goals, objectives, or mission of the agency. What is its impact?
6. Is the disciplinary action being applied consistently? What has been the consequence for other employees committing a similar infraction?
7. What are the consequences? Explain what may happen if the necessary improvement is not made by the specified time or if the act occurs again (i.e., further disciplinary action up to and including dismissal).

V. TYPES OF DISCIPLINARY ACTIONS

- A. The following are disciplinary measures to be considered. Depending upon the severity of offenses, discipline may be implemented at any step determined to be appropriate, without requirement to use it progressively or incrementally. In some instances, immediate dismissal may be warranted.

Written Reprimand: Address the items in Section IV. Reprimands are generally issued under the supervisor's/manager's signature. The subject line of the memo will be, "Written Reprimand." The last line of the memo will state that a copy will be placed in the employee's official file in the OP. Note: See V.B. for instructions on presentation to employee.

Unacceptable Conduct: Address the items in Section IV. This is a letter issued under the Appointing Authority's signature. A request for a Notice of Unacceptable Conduct is



ADMINISTRATIVE MANUAL

SUBJECT: PROBATION, PERFORMANCE APPRAISAL AND DISCIPLINE Disciplinary Action	Chapter: 10
	Section: 10.4
REFERENCES: State Personnel Division Rules Manual – 1 CSR 20-3.070	Page: 5 of 6
RSMo Chapters 36.410 and 577.520, HB 600	Revised: 9-23-03

to be submitted through administrative channels to OP. The OP prepares the letter for the Appointing Authority's signature. The letter will be presented to the employee by the supervisor or manager in a conference. This form of disciplinary action is also entered into the employee's record at the Office of Administration/Division of Personnel. Note: See V.B. for instructions on presentation to employee.

Suspension: Suspension is time away from work without pay. This action is taken by the Appointing Authority. A request for suspension, addressing the items in Section IV, is to be submitted through administrative channels to OP. The OP prepares the notification to the employee for the signature of the Appointing Authority. Note: See V.B. for instructions on presentation to employee.

Involuntary Demotion: This type of disciplinary action may be considered if the employee has previously held regular status in the position they are being demoted to, or are eligible for such position. This action requires the approval of the Appointing Authority, and a request for such action explaining why this is the most viable option shall be submitted through administrative channels to OP. The OP will prepare the notification to the employee for signature of the Appointing Authority. Note: See V.B. for instructions on presentation to employee.

Dismissal: This action is issued only by the Appointing Authority. A request for dismissal, addressing the items in Section IV, is to be submitted through administrative channels to OP. The OP prepares the notification to the employee for signature of the Appointing Authority. In most instances, the original document is given to the employee in a conference. Note: See V.B. for instructions on presentation to employee.

Dismissal Without Prejudice: If the Appointing Authority determines the circumstances warranting dismissal do not reflect discredit on the character or conduct of the employee, he/she may dismiss the employee "without prejudice." This may apply to situations in which an employee was unable to meet expectations due to a medical condition, extensive absences brought on by a medical condition, etc. See V.B. for instructions on presentation to employee.

B. Presentation Instructions:

1. In most instances, the supervisor and/or manager/bureau chief gives the original document to the employee in a conference. The supervisor obtains the employee's



ADMINISTRATIVE MANUAL

SUBJECT: PROBATION, PERFORMANCE APPRAISAL AND DISCIPLINE Disciplinary Action	Chapter: 10
	Section: 10.4
REFERENCES: State Personnel Division Rules Manual – 1 CSR 20-3.070	Page: 6 of 6
RSMo Chapters 36.410 and 577.520, HB 600	Revised: 9-23-03

signature acknowledging receipt and forwards the receipt notice containing original signatures, along with a copy of the disciplinary action, to the OP for the employee's official personnel records.

2. If the employee refuses to sign, the supervisor and one other person sign as witnesses that the employee received the document. The other witness must be a manager/supervisor or confidential secretary to the manager/supervisor. Never use a co-worker as a witness. In some cases, the employee may not be available for personal presentation, in which case the document is sent via certified mail. The return receipt is then sent to OP for inclusion in the employee's official personnel file.
3. An employee shall be entitled to Union or non-Union co-worker representation to provide advice, assistance, or representation upon request if the employee is questioned by an agency representative about a matter that the employee reasonably believes may lead to a notice of unacceptable conduct, a notice of conditional employment, demotion, suspension or dismissal of the employee. Management shall allow approximately fifteen minutes conference time between Union or co-worker representative and employee prior to investigatory/disciplinary meetings. If management is certain that the situation will not result in disciplinary action of the aforementioned magnitude, management can so inform the employee and deny representation.

Prepared by:

Approved by:

Chief, Office of Personnel

Chief Operating Officer

<p>Confidentiality Statement Central Office</p> <p>Missouri Department of Health and Senior Services Office of Surveillance HIV/AIDS SURVEILLANCE PROGRAM</p>
--

EMPLOYEE OATH OF CONFIDENTIALITY:

I hereby acknowledge that I will abide by the appropriate state statutes, regulations, protocols, and policies, regarding the confidentiality and security of HIV/AIDS surveillance data and information. I will not release HIV/AIDS surveillance data or information to any individual not granted authorization by the Missouri Department of Health and Senior Services (MDHSS) Central Office HIV/AIDS surveillance program. I will contact the Chief of the Office of Surveillance, 573/751-9071, for any questions regarding the release of confidential information and to report breaches or suspected breaches of confidentiality. [Appropriate release of information is defined in the *HIV/AIDS Confidentiality and Security Manual*. This manual defines statewide policy and protocols for the security of HIV/AIDS surveillance information.]

Penalties for unauthorized disclosure of confidential data or information are outlined in Missouri statute, RSMo 191.656. In addition to penalties under RSMo 191.656, violation of these standards is subject to disciplinary actions that could include suspension, demotion, or termination (MDHSS Administrative Manual, Chapter 10, Section 10.4).

I have received copies of the *HIV/AIDS Confidentiality and Security Manual*, state statute RSMo 191.656, and the MDHSS administrative rule. I understand the consequences of violating confidentiality of any HIV/AIDS data or information.

Employee Signature and Date

Witness Signature and Date

CONFIDENTIALITY STATEMENT
Missouri Department of Health and Senior Services
Office of Surveillance
HIV/AIDS Surveillance Program

ST. LOUIS CITY DEPARTMENT OF HEALTH AND HOSPITALS
HIV/AIDS SURVEILLANCE PROGRAM

EMPLOYEE OATH OF CONFIDENTIALITY:

I hereby acknowledge that I will abide by the appropriate state statutes, regulations, protocols, and policies regarding the confidentiality and security of HIV/AIDS surveillance data and information. I will not release HIV/AIDS surveillance data or information to any individual not granted authorization by the Missouri Department of Health and Senior Services (MDHSS) Central Office HIV/AIDS surveillance program. I will report local breaches or suspected breaches of confidentiality to the local Overall Responsible Party [ORP] (when designated). The point of contact for any questions regarding release of information is the HIV/AIDS Surveillance Program Manager, Office of Surveillance, 573/751-6463. [Appropriate release of information is defined in the *HIV/AIDS Confidentiality and Security Manual*. This manual defines statewide policy and protocols for the security of HIV/AIDS surveillance information.]

Penalties for unauthorized disclosure of confidential data or information are outlined in Missouri statute, RSMo 191.656. In addition to penalties under RSMo 191.656, violation of these standards is subject to disciplinary actions that could include suspension, demotion, or termination.

I have received copies of the *HIV/AIDS Surveillance Confidentiality Manual*, state statute RSMo 191.656, and the MDHSS administrative rule. I understand the consequences of violating confidentiality of any HIV/AIDS data or information.

Employee Signature and Date

Reviewer Signature and Date

CONFIDENTIALITY STATEMENT
Missouri Department of Health and Senior Services
Office of Surveillance

KANSAS CITY HEALTH DEPARTMENT
HIV/AIDS SURVEILLANCE PROGRAM

EMPLOYEE OATH OF CONFIDENTIALITY:

I hereby acknowledge that I will abide by the appropriate state statutes, regulations, protocols, and policies, regarding the confidentiality and security of HIV/AIDS surveillance data and information. I will not release HIV/AIDS surveillance data or information to any individual not granted authorization by the Missouri Department of Health and Senior Services (MDHSS) Central Office HIV/AIDS surveillance program. I will report local breaches or suspected breaches of confidentiality to the local Overall Responsible Party [ORP] (when designated). The point of contact for any questions regarding release of information is the HIV/AIDS Surveillance Program Manager, Office of Surveillance, 573/751-6463. [Appropriate release of information is defined in the *HIV/AIDS Confidentiality and Security Manual*. This manual defines statewide policy and protocols for the security of HIV/AIDS surveillance information.]

Penalties for unauthorized disclosure of confidential information are outlined in Missouri statute, RSMo 191.656. In addition to penalties under RSMo 191.656, violation of these standards is subject to disciplinary actions that could include suspension, demotion, or termination.

I have received copies of the *HIV/AIDS Surveillance Confidentiality Manual*, state statute RSMo 191.656, and the MDHSS administrative rule. I understand the consequences of violating confidentiality of any HIV/AIDS data or information.

Employee Signature and Date

Reviewer Signature and Date

Confidentiality Statement
Tuberculosis Program

Missouri Department of Health and Senior Services
Office of Surveillance
HIV/AIDS SURVEILLANCE PROGRAM

EMPLOYEE OATH OF CONFIDENTIALITY:

I hereby acknowledge that I will abide by the appropriate state statutes, regulations, protocols, and policies, regarding the confidentiality and security of HIV/AIDS surveillance data and information. I will not release HIV/AIDS surveillance data or information to any individual not granted authorization by the Missouri Department of Health and Senior Services (MDHSS) Central Office HIV/AIDS surveillance program. I will refer any questions regarding release of information to the Chief, Office of Surveillance, 573/751-6463. [Appropriate release of information is defined in the *HIV/AIDS Confidentiality and Security Manual*. This manual defines statewide policy and protocols for the security of HIV/AIDS surveillance information.]

Penalties for unauthorized disclosure of confidential data or information are outlined in Missouri statute, RSMo 191.656. In addition to penalties under RSMo 191.656, violation of these standards is subject to disciplinary actions that could include suspension, demotion, or termination (MDHSS Administrative Manual, Chapter 10, Section 10.4).

I have received copies of RSMo 191.656 and the MDHSS administrative rule. I understand the consequences of violating confidentiality of any HIV/AIDS data or information.

Employee Signature and Date

Witness Signature and Date

Confidentiality Statement
Office of Information Systems

Missouri Department of Health and Senior Services
Office of Surveillance
HIV/AIDS SURVEILLANCE PROGRAM

EMPLOYEE OATH OF CONFIDENTIALITY:

I hereby acknowledge that I will abide by the appropriate state statutes, regulations, protocols, and policies, regarding the confidentiality and security of HIV/AIDS surveillance data and information. I will not release HIV/AIDS surveillance data or information to any individual not granted authorization by the Missouri Department of Health and Senior Services (MDHSS) Central Office HIV/AIDS surveillance program. I will refer any questions regarding release of information to the Chief, Office of Surveillance, 573/751-6463. [Appropriate release of information is defined in the *HIV/AIDS Confidentiality and Security Manual*. This manual defines statewide policy and protocols for the security of HIV/AIDS surveillance information.]

Penalties for unauthorized disclosure of confidential data or information are outlined in Missouri statute, RSMo 191.656. In addition to penalties under RSMo 191.656, violation of these standards is subject to disciplinary actions that could include suspension, demotion, or termination (DHSS Administrative Manual, Chapter 10, Section 10.4).

I have received copies of RSMo 191.656 and the DHSS administrative rule. I understand the consequences of violating confidentiality of any HIV/AIDS data or information.

Employee Signature and Date

Witness Signature and Date

**CERTIFICATION REGARDING COMPLIANCE WITH SECURITY STANDARDS FOR
THE PROTECTION OF HIV/AIDS SURVEILLANCE INFORMATION AND DATA
MISSOURI DEPARTMENT OF HEALTH AND SENIOR SERVICES**

The undersigned has been designated as the overall responsible party (ORP) by the applicant organization. This official accepts overall responsibility for implementing and enforcing the security standards and may be liable for breach of confidentiality. The ORP should be a high-ranking public health official, for example, the division director or department chief over HIV/AIDS surveillance. This official should have the authority to make decisions about surveillance operations that may affect programs outside the HIV/AIDS surveillance unit and should serve as one of the contacts to public health professionals and the HIV affected community on policies and practices associated with HIV/AIDS surveillance.

By signing, the ORP certifies that the applicant will comply with the “*Security Standards for the Protection of HIV/AIDS Surveillance Information and Data*” by:

- (a) Attesting that good faith efforts have been undertaken during fiscal year 2003 to attain all “**Program Requirements**” included in the “*Security Standards for the Protection of HIV/AIDS Surveillance Information and Data*”.
- (b) Acknowledging that attainment of all “**Program Requirements**” is expected by fiscal year 2004.
- (c) Applying the “**Program Requirements**” to all local/state/territorial staff and contractors funded through CDC to perform HIV/AIDS surveillance activities.
- (d) Applying the “**Program Requirements**” at all sites where the HIV/AIDS Reporting System (HARS) is maintained.

Name and address of organization	
Missouri Department of Health and Senior Services Division of Environmental Health and Communicable Disease Prevention 930 Wildwood Drive PO Box 570 Jefferson City, Missouri 65102	
Phone no. (with area code) (573) 751-6080	Fax no. (with area code) (573) 751-6417
Name of ORP (print)	Title
Signature	Date

**CERTIFICATION REGARDING COMPLIANCE WITH SECURITY STANDARDS FOR
THE PROTECTION OF HIV/AIDS SURVEILLANCE INFORMATION AND DATA
MISSOURI DEPARTMENT OF HEALTH AND SENIOR SERVICES**

The undersigned has been designated as the overall responsible party (ORP) by the applicant organization. This official accepts overall responsibility for implementing and enforcing the security standards and may be liable for breach of confidentiality. The ORP should be a high-ranking public health official, for example, the division director or department chief over HIV/AIDS surveillance. This official should have the authority to make decisions about surveillance operations that may affect programs outside the HIV/AIDS surveillance unit and should serve as one of the contacts to public health professionals and the HIV affected community on policies and practices associated with HIV/AIDS surveillance.

By signing, the ORP certifies that the applicant will comply with the “Security Standards for the Protection of HIV/AIDS Surveillance Information & Data” by:

- (a) Attesting that good faith efforts have been undertaken during fiscal year 2003 to attain all “**Program Requirements**” included in the “Security Standards for the Protection of HIV/AIDS Surveillance Information and Data”.
- (b) Acknowledging that attainment of all “**Program Requirements**” is expected by fiscal year 2004 as a condition of receiving federal HIV/AIDS surveillance funding from the Missouri Department of Health and Senior Services.
- (c) Report all breaches or suspected breaches of confidentiality occurring within the Surveillance jurisdiction (as defined in Scope of Work) to statewide ORP (B. McNally) or designate (Chief, Office of Surveillance).
- (d) Adherence to all statewide policy and procedures as outlined in the *HIV/AIDS Confidentiality and Security Manual*.

St. Louis City Department of Health and Hospitals 634 North Grand, Suite 436 St. Louis, Missouri 63103	
Phone no. (with area code)	Fax no. (with area code)
Name of ORP (print)	Title
Signature	Date

Individual Office Security Checklist - HIV/AIDS Surveillance

A. Hard Copy Data

1. All HIV/AIDS data containing patient identifiers are stored in (double) locked storage (e.g., file cabinets with bar locks) when not under current investigation or at the end of each day.
2. Keys to locked file cabinets are securely maintained.
3. Confidential documents are placed out of view or secured when absent from workstations for short periods of time or at the end of each day.
4. Documents containing personal identifiers (e.g., case reports, phone messages) are shredded when no longer needed.

B. PC Data/Workstations

1. Passwords are kept confidential and not recorded in the workstation.
2. Documents containing personal identifiers are stored in appropriate database (i.e., HARS, or other supplemental database) or on confidential drives.
3. Confidential information is not left on-screen when absent from workstation.
4. Screen saver is set for lowest time interval (preferably 1-2 minutes).
5. Staff should log out of network when absent from workstations for extended periods of time (defined as 2 hours) and at the end of each day.
6. All disks containing confidential information is forwarded to the data manager or other authorized personnel for proper erasure (Norton's WipeInfo) when no longer needed.
7. All surplus computers are sent to the data manager for processing and then forwarded to OIS staff to ensure appropriate erasure.

C. Transfer/Release of Data

1. Line listings containing patient information are never released.
2. Names and personal identifiers are used in written correspondence only when necessary; and status not identified, wherever possible.
3. Addressee is informed that confidential correspondence is being faxed, and all correspondence is addressed/sent directly to the correct person. Addressee should be instructed to contact sender if correspondence is not received within the expected timeframe. For facsimile transmission, a dedicated line is used.
4. Staff should assure that confidential information communicated by phone is released only to appropriate authorized personnel and precautions taken to insure that personnel are authorized (e.g., call back verification).
5. Information with personal identifiers should not be left on answering machine or voice mail unless determined to be a secured line.

6. Incoming phone calls are answered generically (e.g., Department of Health and Senior Services, "This is _____").
7. Staff should discuss confidential information only in secure, private areas and be conscious of the environment (e.g., visitors).
8. Small cell information is not released without the authorization of the Program Manager, HIV/AIDS Surveillance.
9. Patient information is not released without the authorization of the Program Manager, HIV/AIDS Surveillance.
10. Confidential information is not left in common work areas (i.e., photocopier, printer, fax).

D. Out-of-Office Security Measures

1. All line listings or written information containing personal identifiers are removed from office only when necessary (i.e., medical record reviews, validation studies), and do not contain direct references to HIV/AIDS.
2. Confidential information is never left unattended.
3. Field activities are conducted in secure and confidential areas as possible.